UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NORTH DAKOTA

Jason Quaife, John Hoffer, Amanda Koffler, Alec R. Kiesow, and Samantha Stock on behalf of themselves individually and all others similarly situated, Plaintiffs, v. Brady, Martz & Associates, P.C., Defendant.	Case No. 3:23-cv-176-PDW-ARS **CONSOLIDATED CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiffs Jason Quaife, John Hoffer, Amanda Koffler, Alec R. Kiesow, and Samantha Stock (collectively, "Plaintiffs"), on behalf of themselves and all others similarly situated (the "Class"), bring this Class Action Complaint against Defendant, Brady, Martz & Associates, P.C. ("Brady Martz" or "Defendant"). The allegations in this Complaint are based on the personal knowledge of the Plaintiffs and upon information and belief and further investigation of counsel.

INTRODUCTION

1. Defendant is an accounting, tax, and audit services firm operating based in Grand Forks, North Dakota, and operating throughout North Dakota and in northwestern Minnesota.

2. Defendant provides its services in a wide range of industries, including agribusiness, communication & electric utilities, construction & real estate, dealerships,

financial institutions, government, healthcare, nonprofit, oil & gas, and tribal & gaming.[1] These services include audit & assurance, business valuation, employee benefit plans, forensic accounting, litigation support, strategic business solutions, succession and exit planning, wealth management, tax services, and technology services.

3. As part of its operations, Defendant collects, maintains, and stores highly sensitive personal information, including, but not limited to: Social Security numbers, dates of birth, full names, addresses, telephone numbers, driver's license numbers ("Personally Identifying Information" or "PII"). Defendant also collects medical information from its clients, including but not limited to treatment information, diagnoses, and prescription information, medical record numbers, health insurance information, and other protected health information ("Private Health Information" or "PHI"). Further, Defendant also collects financial account/payment card information ("Financial Account Information") (collectively, with PII and PHI, "PI").

4. On November 19, 2022, Defendant noticed unusual activity on its networks. It allegedly retained independent cybersecurity specialists to investigate. Defendant's investigations determined that unauthorized cybercriminals accessed its information systems and databases and stole PI belonging to Plaintiffs and approximately 53,524 Class Members (the "Data Breach"). On September 8, 2023, Defendant dispatched data breach

[1] https://www.bradymartz.com/ (last visited Nov. 17, 2023).

notice letters to individuals whose information was accessed in this incident (the "Notice Letter").[2]

5. As Defendant stored and handled such highly sensitive PII, PHI, and financial account information, it assumed legal and equitable duties to safeguard such PI from cybersecurity threats and unauthorized disclosure.

6. Ultimately, Defendant failed to fulfill these obligations as unauthorized cybercriminals breached Defendant's information systems and databases and stole vast quantities of PI belonging to Plaintiffs and Class Members. This Breach and the successful exfiltration of PI were a direct, proximate, and foreseeable result of Defendant's failure to implement and maintain reasonable safeguards; failure to comply with industry-standard data security practices and federal and state laws and regulations governing data security; failure to properly train its employees on data security measures and protocols; and failure to timely recognize and detect unauthorized third parties accessing its system and that substantial amounts of data had been compromised.

7. In addition to the failures that caused the Data Breach, Defendant unreasonably failed to timely notify victims that their PI had been compromised. Defendant learned of the Data Breach on November 19, 2022, yet it did not send Notice Letters to Plaintiffs and Class Members until September 8, 2023. Defendant's inexcusably long delay

[2] This Notice and information packet that Defendant dispatched to the Maine Attorney General, contained further information regarding the data security breach incident. *See* https://apps.web.maine.gov/online/aeviewer/ME/40/9b9f089f-c004-4fa5-a3a7-ad33820bbcd1.shtml (last visited Nov. 17, 2023).

deprived Plaintiffs and Class Members of even an opportunity to mitigate their damages for nearly one year.

8. Defendant made a meager attempt to ameliorate the effects of the Data Breach and its handling of the same with a brief period of complimentary credit monitoring. However, this limited duration of credit monitoring is woefully inadequate given that the victims face a life-long heightened risk of identity theft, and much of the PI stollen is immutable. Defendant also claims to have taken unspecified "steps to prevent such incidents from happening in the future." *See* Notice Letter.

9. As a result of Defendant's failure to adequately satisfy its contractual, statutory, and common-law obligations, Plaintiffs and Class Members suffered injuries including, but not limited to, the following:

- Lost or diminished value of their PI;
- Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PI;
- Lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges;
- Time needed to change usernames and passwords on their accounts;
- Time needed to investigate, correct, and resolve unauthorized access to their accounts; time needed to deal with spam messages and e-mails received after the Data Breach;
- Charges and fees associated with fraudulent charges on their accounts; and the continued and increased risk of compromise to their PI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect it.

10. Accordingly, Plaintiffs bring this action on behalf of all those similarly situated to seek relief for the consequences of Defendant's failure to reasonably safeguard their and Class Members' PI; its failure to reasonably provide timely notification that Plaintiffs and Class Members' PI had been compromised by an unauthorized third party; and for intentionally and unconscionably deceiving Plaintiffs and Class Members concerning the status, safety, location, access, and protection of their PI.

PARTIES

11. Plaintiff Jason Quaife is and was at all relevant times a citizen of Minnesota and currently resides in Moorhead, Minnesota. Plaintiff Quaife received Defendant's September 8, 2023, Notice of Data Breach letter from Defendant nearly eleven months after the Data Breach was detected in November 2022. On information and belief, Plaintiff's PI was provided to Defendant through his previous employment as a contract Security/Event Ambassador with the City of Fargo, North Dakota in 2015.

12. Plaintiff John Hoffer is and at all relevant times was a citizen of Massachusetts and currently resides in Brookline, Massachusetts. On or about September 13, 2023, Plaintiff Hoffer was informed via Defendant's September 8, 2023, Notice of Data Breach that he had been a victim of the Data Breach.

13. Plaintiff Amanda Koffler is and at all relevant times was a resident and citizen of Dickinson, North Dakota. On September 12, 2023, Plaintiff Koffler received Defendant's Data Breach Notice which explained that information such as her name, date of birth, driver's license or state ID number, health information, medical information, and

Social Security number were compromised in the Data Breach. Prior to receiving this notice, she was unaware that Defendant possessed her PI.

14. Plaintiff Alec Kiesow is and at all relevant times was a citizen of Minnesota and currently resides in Goodridge, Minnesota. Plaintiff Kiesow received Defendant's September 8, 2023, Notice of Data Breach letter from Defendant nearly eleven months after the Data Breach was first detected in November 2022.

15. Plaintiff Samantha Stock is and was at all relevant times a citizen of Minnesota and currently resides in Silver Bay, Minnesota. Plaintiff Stock received Defendant's September 8, 2023, Notice of Data Breach letter from Defendant nearly eleven months after the Data Breach was first detected in November 2022 indicating that her data had "been accessed by the unauthorized party" and could have "included your name and Social Security Number." She immediately took preventative steps to protect her credit and reported such incident to the Federal Trade Commission along with directly contacting Defendant to attempt to determine how it had access to her PI.

16. Defendant Brady, Martz & Associates, P.C. is a professional corporation formed under the laws of the State of North Dakota and Minnesota, with its principal place of business located at 401 Demers Avenue, Suite 300, Grand Forks, North Dakota.

JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the aggregate amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than

100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

18. This Court has personal jurisdiction over Defendant as Defendant's principal place of business is located within this District.

19. Venue is proper in this Court under 28 U.S.C. § 1391, because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District, and Defendant resides within this judicial district.

FACTUAL ALLEGATIONS

Background

20. In the ordinary course of doing business with Defendant, customers, and prospective customers are required to provide Defendant with sensitive PI[3] of themselves and other individuals such as:

a. Full names;

b. Social Security numbers;

c. Driver's license numbers;

d. Passport numbers;

e. Government identification numbers;

f. Dates of birth;

g. Financial account information.

[3] The North Dakota Century Code defines "personal information" as "an individual's first name or first initial and last name in combination with any of the following data elements, when the name and the data elements are not encrypted . . . (1) The individual's social security number." *See* N.D.C.C. § 51-30 (4)(a) (listing data elements (1)–(10)).

21. Defendant Brady Martz, provides a privacy policy on its website, wherein it states that it "is committed to maintain the privacy of information related to its clients, customers and consumers that it collects and maintains as a result of its business practices."[4] Defendant further states that, to guard this information, it "maintains physical, electronic and procedural safeguards that comply with our professional standards."

The Data Breach

22. As stated in its disclosure to the Maine Attorney General, Defendant became aware of "unusual activity" in its "digital environment" on November 19, 2022.

23. Brady Martz then allegedly took steps to secure its systems and retain independent cybersecurity experts to investigate the matter further. It was not purported until August 31, 2023, that Brady Martz determined that personal information was implicated in the incident.

24. In disclosures to the Maine Attorney General, Defendant stated that the Data Breach was discovered on November 19, 2022.[5]

25. However, despite first learning of the Data Breach on or about November 19, 2022, Defendant did not take any steps to notify affected Class Members until at least August 31, 2023.

26. Additionally, though Plaintiffs and Class Members have an interest in ensuring that their information remains protected, the details of the root cause of the Data

[4] https://www.bradymartz.com/privacy-policy (last visited Nov. 17, 2023).

[5] *Supra*, fn.2.

Breach, the vulnerabilities exploited, and the remedial measures taken to ensure a breach does not occur again have not been shared with regulators or Class Members.

Defendant Was Aware of the Data Breach Risks

27. Defendant had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class Members, to keep their PI confidential and to protect it from unauthorized access and disclosure.

28. Plaintiffs and Class Members provided their PI to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with their obligations to employ reasonable care to keep such information confidential and secure from unauthorized access.

29. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches in the banking/credit/financial services industry preceding the date of the Data Breach.

30. Indeed, data breaches, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and completely foreseeable to anyone in Defendant's industry, including Defendant.

31. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and

patience to resolve.[6] Identity thieves use the stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[7]

32. The PI of Plaintiffs and Class Members were taken by cyber criminals for the very purpose of engaging in identity theft, or to sell it to other criminals who will purchase the PI for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years, but the threat is real and imminent.

33. Defendant knew, or reasonably should have known, of the importance of safeguarding the PI of Plaintiffs and Class Members, including Social Security numbers, driver's license numbers and/or state identification numbers, and of the foreseeable consequences that would occur if Defendant's data security systems were breached, including, specifically, the significant costs and emotional toll that would be imposed on Plaintiffs and Class Members as a result of a breach.

34. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiffs and Class members

---

[6] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013), https://www.myoccu.org/sites/default/files/pdf/taking-charge-1.pdf (last visited Nov. 24, 2021).

[7] *Id*. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

are incurring and will continue to incur such damages in addition to any fraudulent use of their PI.

35. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's own failure to implement or maintain adequate data security measures for the PI of Plaintiffs and Class Members.

Defendant Failed to Comply with FTC Guidelines

36. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

37. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their networks' vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

38. The FTC further recommends that companies not maintain PI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for

suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

39. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

40. Defendant failed to properly implement basic data security practices, and its failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PI constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

41. To prevent and detect cyber-attacks, including the attack that resulted in the Data Breach, Defendant should have reasonably taken, as recommended by the United States Government, the following measures:

a. Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of malware and how it is delivered;

b. Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing;

c. Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users;

d. Configure firewalls to block access to known malicious IP addresses;

e. Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system;

f. Set anti-virus and anti-malware programs to conduct regular scans automatically;

g. Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary;

h. Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares;

i. Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications;

j. Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common malware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder;

k. Consider disabling Remote Desktop protocol (RDP) if it is not being used;

l. Use application whitelisting, which only allows systems to execute programs known and permitted by security policy;

m. Execute operating system environments or specific programs in a virtualized environment; and

n. Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

42. Defendant was at all times fully aware of its obligation to protect the PI of customers, prospective customers and employees. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Failed to Comply with Industry Standards

43. A number of industry and national best practices have been published and should have been used as a go-to resources and authoritative guides when developing Defendant's cybersecurity practices. Best cybersecurity practices that are standard in the financial services industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

44. Upon information and belief, Defendant failed to meet the minimum standards of the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness. These frameworks are existing and applicable industry standards in Defendant's industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber-attack and causing the Data Breach.

45. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach.

PI Holds Value to Cyber Criminals

46. Businesses, such as Defendant, that store PI are likely to be targeted by cyber criminals. Credit card and bank account numbers may be tempting targets for hackers, but information such as dates of birth, driver's license and Social Security numbers are even more attractive to cyber criminals; they are not easily destroyed and can be easily used to perpetrate identity theft and other types of fraud.

47. The PI of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[8]

48. Social Security numbers, for example, are among the worst kinds of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration ("SSA") stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number

[8] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web- how-much-it-costs (last visited Apr. 7, 2021).

> and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems. [9]

49. It is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

50. Furthermore, as the SSA warns:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[10]

---

[9] *Identity Theft and Your Social Security Number*, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Nov. 24, 2021).

[10] *Id.*

51. Here, the unauthorized access left the cyber criminals with the tools to perform the most thorough identity theft—they have obtained all the essential PI to mimic the identity of the user. The personal data of Plaintiffs and Class Members stolen in the Data Breach constitutes a dream for hackers and a nightmare for Plaintiffs and Class Members. The stolen personal data of Plaintiffs and Class Members represents essentially one-stop shopping for identity thieves.

52. The FTC has released its updated publication on protecting PI for businesses, which includes instructions on protecting PI, properly disposing of PI, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

53. General policy reasons support such an approach. A person whose personal information has been compromised may not see any signs of identity theft for years. According to the United States Government Accountability Office ("GAO") Report to Congressional Requesters:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[11]

54. Companies recognize that PI is a valuable asset and a valuable commodity. A "cyber black-market" exists in which criminals openly post stolen Social Security

[11] *See Report to Congressional Requesters*, Government Accountability Office, https://www.gao.gov/assets/gao-07-737.pdf (June 2007) at 29.

numbers and other PI on a number of Internet websites. The stolen personal data of Plaintiffs and Class Members has a high value on both legitimate and black markets.

55. Identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, and/or using the victim's information to obtain a fraudulent tax refund or fraudulent unemployment benefits. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

56. As noted above, the disclosure of Social Security numbers in particular poses a significant risk. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns. Class Members whose Social Security numbers have been compromised now face a real, present, imminent and substantial risk of identity theft and other problems associated with the disclosure of their Social Security number and will need to monitor their credit and tax filings for an indefinite duration.

57. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because those victims can cancel or close credit and debit card accounts. The static information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number, driver's license number or government-issued identification number, name, and date of birth are durable.

58. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card

information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[12]

59. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police. An individual may not know that his or her driver's license was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud, or until the individual attempts to lawfully apply for unemployment and is denied benefits (due to the prior, fraudulent application and award of benefits).

Plaintiffs' and Class Members' Damages

60. Defendant has failed to provide any compensation for the unauthorized release and disclosure of Plaintiffs and Class Members' PI other than offering 12 months of "complimentary identity protection services to individuals whose Social Security numbers were affected by the incident."

61. Plaintiffs and Class Members have been damaged by the compromise of their PI in the Data Breach.

62. Plaintiffs and Class Members presently face an imminent and substantial risk of out-of-pocket fraud losses such as loans opened in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

[12] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem- hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Apr. 7, 2021).

63. Plaintiffs and Class Members have been, and currently face substantial and imminent risk of being targeted now and in the future, subjected to phishing, data intrusion, and other illegality based on their PI as potential fraudsters could use that information to target such schemes more effectively to Plaintiffs and Class Members.

64. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

65. Plaintiffs and Class Members also suffered a loss of value of their PI when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in data breach cases.

66. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time monitoring their financial accounts and records for misuse.

67. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

68. Moreover, Plaintiffs and Class Members have an interest in ensuring that their PI, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password protected.

69. Further, as a result of Defendant's conduct, Plaintiffs and Class Members are forced to live with the anxiety that their PI—which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

70. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

Plaintiff Quaife's Experience

71. Plaintiff Quaife entrusted his PI and other confidential information to an employer with the reasonable expectation and understanding that the employer and its vendor Defendant would take, at a minimum, industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify him of any data security incidents related to his PI. Plaintiff Quaife would not have entrusted his PI to his employer, who subsequently retained Defendant's financial services, had he known that Defendant would not take reasonable steps to safeguard his sensitive PI.

72. Plaintiff Quaife has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, which include spending time on the telephone calls, researching the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts. This is time that has been lost forever and cannot be recaptured.

73. Plaintiff Quaife stores all documents containing his PI in a safe and secure location. Moreover, he diligently chooses unique usernames and passwords for the few online accounts that he has.

74. Plaintiff Quaife has suffered actual injury in the form of damages to, and diminution in, the value of his PI—a form of intangible property that Plaintiff Quaife entrusted to Defendant. This PI was compromised in, and has been diminished as a result of, the Data Breach.

75. Plaintiff Quaife has also suffered actual injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a result of the Data Breach, and has anxiety and increased concerns due to the loss of his privacy and the substantial risk of fraud and identity theft which he now faces.

76. Plaintiff Quaife has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his PI resulting from the compromise of his PI, especially his Social Security number, in combination with his name, address, phone number, and email address, which PI is now in the hands of cyber criminals and other unauthorized third parties.

77. Knowing that thieves stole his PI, including his Social Security number and/or driver's license number and other PI that he was required to provide to Defendant through his employer, and knowing that his PI will likely be sold on the dark web, has caused Plaintiff Quaife great anxiety.

78. Additionally, Plaintiff Quaife does not recall having been involved in any other data breaches in which his highly confidential PI, such as his Social Security Number, was compromised.

79. Plaintiff Quaife has a continuing interest in ensuring that his PI which, upon information and belief, remains in the possession of Defendant, is protected and safeguarded from future data breaches.

80. As a result of the Data Breach, Plaintiff Quaife is presently and will continue to be at a present and heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Hoffer's Experience

81. On or about September 13, 2023, Plaintiff was notified via a physical letter (dated September 8, 2023) from Defendant that he had been the victim of the Data Breach.

82. Plaintiff is uncertain of exactly how Defendant came to be in possession of his PI, as Plaintiff (to the best of his knowledge) has never directly used Defendant's services. However, Plaintiff believes that his local bank likely provided Defendant with his PI.

83. Additionally, Plaintiff has already spent more than 10 hours of time he would otherwise have spent on other tasks contacting (or attempting to contact) his bank, former medical services providers, and the number provided by Defendant in its notice letter regarding exactly what information was lost and who provided that information to Defendant.

84. Given that Plaintiff believes his bank to have been the source of his PI, Plaintiff closed out his account with his bank, which included closing out a certificate of deposit at his bank, which led to him losing some accrued interest due to the early withdrawal.

85. Plaintiff is aware of no other source from which the theft of his PI could have come. He regularly takes steps to safeguard his own PI in his own control.

Plaintiff Koffler's Experience

86. Plaintiff Amanda Koffler does not know how Defendant acquired her PI. On information and belief, her PI was provided to Defendant by an entity that was a client of Defendant.

87. On or about September 8, 2023, Plaintiff Koffler received Defendant's data breach notice. The notice informed her that her name and Social Security number were exposed in the data breach.

88. Plaintiff Koffler experienced a massive uptick in the number of spam calls and emails which started in December 2022 or January 2023 and continues to the present day. Given the timeline of the breach, Plaintiff Koffler believes that this dramatic uptick in spam is the result of the Data Breach.

89. Plaintiff Koffler has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, which include spending time on the telephone calls, researching the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts. This is time that has been lost forever and cannot be recaptured.

90. Plaintiff Koffler stores all documents containing her PI in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for the few online accounts that she has.

91. Plaintiff Koffler has suffered actual injury in the form of damages to, and diminution in, the value of her PI—a form of intangible property that was entrusted to Defendant. This PI was compromised in, and has been diminished as a result of, the Data Breach.

92. Plaintiff Koffler has also suffered actual injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a result of the Data Breach, and has anxiety and increased concerns due to the loss of her privacy and the substantial risk of fraud and identity theft which she now faces.

93. Plaintiff Koffler has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of her PI resulting from the compromise of her PI, especially her Social Security number.

94. Knowing that thieves stole her PI, including her Social Security number and potentially other PI that was provided to Defendant, and knowing that her PI will likely be sold on the dark web, has caused Plaintiff Koffler great anxiety.

95. Additionally, Plaintiff Koffler does not recall having been involved in any other data breaches in which her highly confidential PI, such as her Social Security Number, was compromised.

96. Plaintiff Koffler has a continuing interest in ensuring that her PI which, upon information and belief, remains in the possession of Defendant, is protected and safeguarded from future data breaches.

97. As a result of the Data Breach, Plaintiff Koffler is presently and will continue to be at a present and heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Kiesow's Experience

98. Plaintiff Kiesow entrusted his PII and other confidential information to Defendant with the reasonable expectation and understanding that Defendant or its agents, would take industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify him of any data security incidents related to his PII. Plaintiff Kiesow would not have allowed Defendant's financial services to collect and maintain his PII had he known that Defendant would not take reasonable steps to safeguard his PII.

99. Plaintiff Kiesow has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, which include spending time on the telephone calls, researching the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts. This is time that has been lost forever and cannot be recaptured.

100. Plaintiff Kiesow stores all documents containing his PII in a safe and secure location. Moreover, he diligently chooses unique usernames and passwords for the online accounts that he has.

101. Plaintiff Kiesow has suffered actual injury in the form of damages to, and diminution in, the value of his PII, a form of intangible property that Plaintiff Kiesow entrusted to Defendant. This PII was compromised in, and has been diminished as a result of, the Data Breach.

102. Plaintiff Kiesow has also suffered actual injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a result of the Data Breach, and has anxiety and increased concerns due to the loss of his privacy and the substantial risk of fraud and identity theft which he now faces.

103. Plaintiff Kiesow has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his PII resulting from the compromise of his PII, especially his Social Security number, in combination with his name, address, phone number, and email address, which PII is now in the hands of cyber criminals and other unauthorized third parties.

104. Knowing that thieves stole his PII, including his Social Security number and/or driver's license number and other PII that he was required to provide to Defendant through his employer, and knowing that his PII will likely be sold on the dark web, has caused Plaintiff Kiesow great anxiety.

105. Additionally, Plaintiff Kiesow does not recall having been involved in any other data breaches in which his highly confidential PII, such as Social Security Number was compromised.

106. Plaintiff Kiesow has a continuing interest in ensuring that his PII which, upon information and belief, remains in the possession of Defendant, is protected and safeguarded from future data breaches.

107. As a result of the Data Breach, Plaintiff Kiesow is presently and will continue to be at a present and heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Stock's Experience

108. Plaintiff Stock entrusted her PI and other confidential information to a previous employer with the reasonable expectation and understanding that the employer and its vendor Defendant would take, at a minimum, industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify him of any data security incidents related to his PI. Plaintiff Stock would not have entrusted her PI to an employer, who subsequently retained Defendant's financial services, had she known that Defendant would not take reasonable steps to safeguard her sensitive PI.

109. Plaintiff Stock has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, which include spending time on the telephone calls, researching the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts.

110. Plaintiff Stock contacted the Federal Trade Commission on September 13, 2023, after she had received Defendant's data breach notice letter to report the incident. She also reached out directly to Defendant and spoke on the phone with an individual from

Brady Martz on September 14, 2023, to inquire as to how Defendant had gained possession of her PI and was told that it was likely a former employer but would not divulge further information. This is time that has been lost forever and cannot be recaptured.

111. Plaintiff Stock also discovered that a land transaction that she had no knowledge of showed up on her credit report when pulled by a creditor and believes it is a direct result of the Data Breach.

112. Plaintiff Stock stores all documents containing her PI in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for the few online accounts that she has.

113. Plaintiff Stock has suffered actual injury in the form of damages to, and diminution in, the value of her PI—a form of intangible property that Plaintiff Stock entrusted to Defendant through a former employer. This PI was compromised in, and has been diminished as a direct result of, the Data Breach.

114. Plaintiff Stock has also suffered actual injury in the form of lost time and opportunity costs, annoyance, interference, and inconvenience as a result of the Data Breach, and has anxiety and increased concerns due to the loss of his privacy and the substantial risk of fraud and identity theft which she now faces.

115. Plaintiff Stock has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, misuse of her PI, and unauthorized financial activity on her credit report resulting from the compromise of her PI, especially her Social Security number, in combination with her name, which PI is now in the hands of cyber criminals and other unauthorized third parties.

116. Knowing that thieves stole his PI, including her Social Security number and other PI that she was required to provide to Defendant through an employer, and knowing that her PI will likely be sold on the dark web, has caused Plaintiff Stock great anxiety and consternation.

117. Additionally, Plaintiff Stock does not recall having been involved in any other data breaches in which her highly confidential PI, such as her Social Security Number, was compromised.

118. Plaintiff Stock has a continuing interest in ensuring that her PI which, upon information and belief, remains in the possession of Defendant, is protected and safeguarded from future data breaches.

119. As a result of the Data Breach, Plaintiff Stock is presently and will continue to be at a present and heightened imminent risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

CLASS ALLEGATIONS

120. Plaintiffs bring this class action pursuant to Federal Rules of Civil Procedure, Rules 23(b)(2), 23(b)(3), and 23(c)(4), individually and on behalf of all members of the following class:

> All natural persons residing in the United States whose PI was compromised in the Data Breach announced by Defendant on or about September 8, 2023 (the "Class").

121. Plaintiff Hoffer also brings this action on behalf of all members of the following subclass:

> All natural persons residing in Massachusetts whose PI was compromised in the Data Breach announced by Defendant on or about September 8, 2023 (the "Massachusetts Subclass").

122. Plaintiff Koffler also brings this action on behalf of all members of the following subclass:

> All natural persons residing in North Dakota whose PI was compromised in the Data Breach announced by Defendant on or about September 8, 2023 (the "North Dakota Subclass").

123. Excluded from the Class and Subclasses are all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, and all judges assigned to hear any aspect of this litigation and their immediate family members.

124. Plaintiffs reserve the right to modify or amend the definitions of the proposed Class before the Court determines whether certification is appropriate.

125. **Numerosity**. The Class is so numerous that joinder of all members is impracticable. It is estimated that more than 53,000 individuals have had their PI obtained by unauthorized third parties as part of the Data Breach.[13] The exact number of Class Members is in the possession and control of Defendant and will be ascertainable through discovery.

126. **Commonality.** There are numerous questions of law and fact common to Plaintiffs and Class Members that predominate over any questions that may affect only individual Class Members, including, without limitation:

[13] https://apps.web.maine.gov/online/aeviewer/ME/40/9b9f089f-c004-4fa5-a3a7-ad33820bbcd1.shtml (last visited Nov. 17, 2023).

a. Whether Defendant unlawfully maintained, lost or disclosed Plaintiffs and Class Members' PI;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their PI;

f. Whether Defendant breached duties to Class Members to safeguard their PI;

g. Whether cyber criminals obtained Class Members' PI in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Defendant owed a duty to provide Plaintiffs and Class Members timely notice of this Data Breach, and whether Defendant breached that duty;

j. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

k. Whether Defendant's conduct was negligent;

l. Whether Defendant's conduct violated federal law;

m. Whether Defendant's conduct violated state law; and

n. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

127. **Typicality**. Plaintiffs' claims are typical of the claims of the Class in that Plaintiffs, like all Class Members, had their personal data compromised, breached, and stolen in the Data Breach. Plaintiffs and all Class Members were injured through the uniform misconduct of Defendant, described throughout this Complaint, and assert the same claims for relief.

128. **Adequacy**. Plaintiffs and their counsel will fairly and adequately protect the interests of the Class. Plaintiffs retained counsel who are experienced in Class action and complex litigation. Plaintiffs have no interests that are antagonistic to, or in conflict with, the interests of other Class Members.

129. **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action, most Class Members would find the cost of litigating their claims prohibitively high and would therefore have no effective remedy, so that in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the Class. Plaintiffs and Class Members have been harmed by Defendant's wrongful conduct and/or action. Litigating this action as a class action will reduce the possibility of repetitious litigation relating to Defendant's conduct and/or inaction. Plaintiffs know of no difficulties that would be encountered in this litigation that would preclude its maintenance as a class action.

130. Class certification is appropriate under Fed. R. Civ. P. 23(b)(1)(A), in that the prosecution of separate actions by the individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action conserves judicial resources and the parties' resources and protects the rights of each Class Member. Specifically, injunctive relief could be entered in multiple cases, but the ordered relief may vary, causing Defendant to have to choose

between differing means of upgrading its data security infrastructure and choosing the court order with which to comply. Class action status is also warranted because prosecution of separate actions by Class Members would create the risk of adjudications with respect to individual Class Members that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

131. Class certification, therefore, is appropriate under Rule 23(a) and (b)(2) because Defendant has acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

132. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PI;

b. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PI;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and

e. Whether Plaintiffs and Class Members are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Rule 23 Class)

133. Plaintiffs re-allege and incorporate by reference all of the previous allegations contained herein.

134. Plaintiffs and Class Members entrusted Defendant with their PI as a condition of receiving services from Defendant.

135. Plaintiffs and Class Members entrusted their PI to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PI for business purposes only, and not disclose their PI to unauthorized third parties.

136. Defendant owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, using, and protecting their PI from unauthorized third parties.

137. The legal duties owed by Defendant to Plaintiffs and Class Members include, but are not limited to the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PI of Plaintiffs and Class Members in their possession;

b. to protect PI of Plaintiffs and Class Members in their possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiffs and Class Members of the Data Breach.

138. Defendant's duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a) (the "FTC Act"), which prohibits "unfair . . . practices in or affecting commerce," including, as interested and enforced by the Federal Trade Commission, the unfair practices by companies such as Defendant of failing to use reasonable measures to protect PI.

139. Various FTC publications and data security breach orders further form the basis of Defendant's duty. Plaintiffs and Class Members are consumers under the FTC Act. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PI and by not complying with industry standards.

140. Defendant breached its duties to Plaintiffs and Class Members. Defendant knew or should have known the risks of collecting and storing PI and the importance of maintaining secure systems, especially in light of the fact that data breaches have recently been prevalent.

141. Defendant knew or should have known that its security practices did not adequately safeguard the PI of Plaintiffs and Class Members.

142. Through Defendant's acts and omissions described in this Complaint, including Defendant's failure to provide adequate security and its failure to protect the PI of Plaintiffs and Class Members from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the PI of Plaintiffs and Class Members during the period it was within Defendant's possession and control.

143. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and Class Members through close proximity in its business relationship with its financial clients. That special relationship arose because Plaintiffs and Class Members entrusted Defendant with their confidential PI, a necessary part of obtaining services from Defendant.

144. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff.

145. Defendant's own conduct created a foreseeable risk of harm to a foreseeable individual, including Plaintiffs and Class Members. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for safekeeping of the PI of Plaintiffs and Class Members, including basic encryption techniques freely available to Defendant.

146. Defendant was in a position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

147. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination or exfiltration of the PI of Plaintiffs and Class Members.

148. Defendant breached the duties it owes to Plaintiffs and Class Members in several ways, including:

a. Failing to implement adequate security systems, protocols, and practices sufficient to protect employees' and customers' PI and thereby creating a foreseeable risk of harm;

b. Failing to comply with the minimum industry data security standards during the period of the Data Breach;

c. Failing to act despite knowing or having reason to know that its systems were vulnerable to attack; and

d. Failing to timely and accurately disclose to customers and employees that their PI had been improperly acquired or accessed and was potentially available for sale to criminals on the dark web.

149. There is a close causal connection between Defendant's failure to implement security measures to protect the PI of Plaintiffs and Class Members and the harm, or risk of imminent harm, suffered by Plaintiffs and Class Members. The PI of Plaintiffs and Class Members was stolen and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PI by not adopting, implementing, or maintaining appropriate security measures.

150. Due to Defendant's conduct, Plaintiffs and Class Members are entitled to extended credit monitoring and further damages. The PI taken can be used for identity theft and other types of financial fraud against Plaintiffs and Class Members.

151. Some experts recommend that data breach victims obtain credit monitoring services for at least ten years following a data breach. Annual subscriptions for credit monitoring plans range from approximately $219 to $358 per year. To date, Defendant has only offered "12 months of complimentary identity monitoring services."

152. As a result of Defendant's negligence, Plaintiffs and Class Members suffered injuries that include:

a. the lost or diminished value of PI;

b. out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PI;

c. lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including, but not limited to, time spent deleting phishing email messages and cancelling credit cards believed to be associated with the compromised account;

d. the continued risk to their PI, which may remain for sale on the dark web and is in Defendant's possession and subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the PI in their continued possession; and

e. future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class Members, including ongoing credit monitoring.

153. These injuries were reasonably foreseeable given the history of security breaches of this nature in the financial sector. The injury and harm that Plaintiffs and Class Members suffered was the direct and proximate result of Defendant's negligent conduct.

COUNT II
Negligence Per Se
(On Behalf of Plaintiffs and the Rule 23 Class)

154. Plaintiffs re-allege and incorporate by reference all of the previous allegations contained herein.

155. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PI. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

156. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PI and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PI it obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendant's nature, including, specifically, the immense damages that would result to Plaintiffs and Class Members due to the valuable nature of the PI at issue in this case—including Social Security numbers.

157. Defendant's violations of Section 5 of the FTC Act constitute negligence *per se*.

158. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

159. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and Class Members.

160. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to:

a. actual identity theft;

b. the compromise, publication, and/or theft of their PI;

c. out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PI;

d. lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft;

e. costs associated with placing freezes on credit reports;

f. the continued risk to their PI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PI of its current and former employees and customers in its continued possession; and

g. future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PI compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

161. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class Members have suffered and will suffer the continued risks of exposure of their PI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PI in its continued possession.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiffs and the Rule 23 Class)

162. Plaintiffs re-allege and incorporate by reference all of the previous allegations contained herein.

163. Defendant benefited from receiving Plaintiffs and Class Members' PI by its ability to retain and use that information for its own financial business benefit. Defendant understood this benefit.

164. Defendant also understood and appreciated that Plaintiffs and Class Members' PI was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that PI.

165. Plaintiffs and Class Members conferred a monetary benefit upon Defendant in the form of monies paid to Defendant for services.

166. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and Class Members. Defendant also benefited from the receipt of Plaintiffs and Class Members' PI, as Defendant used it in the course of its business.

167. The monies paid to Defendant for services involving Plaintiffs and Class Members' PI were to be used by Defendant, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

168. Defendant also understood and appreciated that Plaintiffs and Class Members' PI was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that PI.

169. But for Defendant's willingness and commitment to maintain privacy and confidentiality, that PI would not have been transferred to and untrusted with Defendant. Indeed, if Defendant had informed its customers that Defendant's data and cyber security measures were inadequate, Defendant would not have been permitted to continue to operate in that fashion by regulators, its shareholders, and its consumers.

170. As a result of Defendant's wrongful conduct, Defendant has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and Class Members.

Defendant continues to benefit and profit from their retention and use of the PI while its value to Plaintiffs and Class Members has been diminished.

171. Defendant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged in this complaint, including compiling, using, and retaining Plaintiffs and Class Members' PI, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

172. As a result of Defendant's conduct, Plaintiffs and Class Members suffered actual damages in an amount equal to the difference in value between the amount the value of their PI prior to and after the Data Breach.

173. Under principals of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiffs and Class Members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

174. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds it received as a result of the conduct alleged herein.

COUNT IV
Declaratory Judgment
(On Behalf of Plaintiffs and the Rule 23 Class)

175. Plaintiffs re-allege and incorporate by reference all of the previous allegations contained herein.

176. Defendant owed duties of care to Plaintiffs and Class Members which require it to adequately secure their PI.

177. Defendant still possess Plaintiffs and Class Members' PI.

178. Defendant does not specify in the Notice of Data Breach letters what steps they have taken to prevent a data breach from occurring again.

179. Plaintiffs and Class Members are at risk of harm due to the exposure of their PI and Defendant's failure to address the security failings that lead to such exposure.

180. Plaintiff, therefore, seeks a declaration that (1) each of Defendant's existing security measures do not comply with their explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect customers' personal information, and (2) to comply with their explicit or implicit contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Conducting regular database scanning and security checks;

f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

g. Purchasing credit monitoring services for Plaintiffs and Class Members for a period of ten years; and

h. Meaningfully educating Plaintiffs and Class Members about the threats they face as a result of the loss of their PI to third parties, as well as the steps they must take to protect themselves.

COUNT V
Violation of the Massachusetts Consumer Protection Act
Mass. Gen. Laws ch. 93a § 1 *et seq.*
(On Behalf of Plaintiff Hoffer and the Massachusetts Subclass)

181. Plaintiffs re-allege and incorporate by reference all of the previous allegations contained herein.

182. Defendant engaged in unfair or deceptive acts and practices by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Massachusetts Subclass members' PI with knowledge that that information would not be adequately protected; and by storing such information in an unsecure electronic environment. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Massachusetts Subclass members. Defendant's actions and representations were likely to deceive the public into believing that their PI would be securely stored when it was not.

183. As a direct and proximate result of Defendant's unfair practices, Massachusetts Subclass members lost money or property, including those alleged above. This harm outweighs the utility of Defendant's unfair practices, if any.

184. Defendant knew or should have known that their cybersecurity measures were insufficient to safeguard Massachusetts Subclass members PI and that a data breach was likely to occur. Defendant's unlawful acts were negligent, reckless, and/or knowing.

185. Plaintiff Hoffer, on behalf of himself and the Massachusetts Subclass, seeks relief under Mass. Gen. Laws. 93a § 1, *et seq.*, including, but not limited to, restitution of money or property Defendant acquired through its unfair practices, statutory and actual damages, double or treble damages, declaratory relief, attorneys' fees and costs, and injunctive or other equitable relief.

COUNT VI
Violation of N.D. Cent. Code § 51-22-02
(On Behalf of the Class or, in the alternative, on Behalf of Plaintiff Koffler and the North Dakota Subclass)

186. Plaintiffs re-allege and incorporate by reference all of the previous allegations contained herein.

187. North Dakota Century Code § 51-22-02 provides: "No business entity which charges a fee for data processing services performed may disclose in whole or in part the contents of any record . . . which is prepared or maintained by such business entity to any person, other than the individual or business entity which is the subject of the record, without the express written consent of such individual or business entity."

188. Defendant is a business entity because it is a corporation doing business in North Dakota. Defendant also charges a fee for, *inter alia*, performing "systematic sequence[s] of operations, including but not limited to bookkeeping functions, inventory control, storage, or manipulation and retrieval of management or personnel information."

N.D. Cent. Code § 51-22-01. These actions are performed "upon data by electronic devices which perform logical, arithmetic, and memory functions by the manipulation of electronic or magnetic impulses." *Id.*

189. Defendant disclosed Plaintiffs and Class Members' PI to third parties without their consent by failing to take appropriate measures to safeguard and protect that PI amidst a foreseeable risk of a cybersecurity attack, resulting in the Data Breach.

190. The damages, ascertainable losses and injuries, including to their money or property, suffered by Plaintiffs and Class Members as a direct result of Defendant's deceptive acts and practices as set forth herein include, without limitation:

a. actual identity theft;

b. the compromise, publication, and/or theft of their PI;

c. out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PI;

d. lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft;

e. costs associated with placing freezes on credit reports;

f. the continued risk to their PI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PI of its current and former employees and customers in its continued possession; and

g. future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PI compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

191. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members suffered actual damages as a result of violations of N.D.C.C. § 51-22-02 and Defendant is thus liable in an amount equal to the actual damages sustained, but in no case less than five hundred dollars to each Plaintiff and Class Member, including but not limited to the damages set forth herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all Class Members, request judgment against Defendant and that the Court grant the following:

1. An order certifying the Class and Subclasses as defined herein, and appointing Plaintiffs and their counsel to represent the Class and their respective Subclasses;
2. An order enjoining Defendant from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of the PI belonging to Plaintiffs and Class Members;
3. An order requiring Defendant to:
    a. Engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
    b. Engage third-party security auditors and internal personnel to run automated security monitoring;
    c. Audit, test, and train its security personnel regarding any new or modified procedures;

d. Segment their user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Conduct regular database scanning and security checks;

f. Routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

g. Purchase credit monitoring services for Plaintiffs and Class Members for a period of ten years; and

h. Meaningfully educate Plaintiffs and Class Members about the threats they face as a result of the loss of their PI to third parties, as well as the steps they must take to protect themselves.

4. An order instructing Defendant to purchase or provide funds for credit monitoring services for Plaintiffs and all Class Members;

5. An award of compensatory, statutory, nominal and punitive damages, in an amount to be determined at trial;

6. An award for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

7. An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable by law; and

8. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand this matter be tried before a jury.

Respectfully Submitted,

November 20, 2023

/s/ Scott Haider
Scott Haider (ND #07533)

SCHNEIDER LAW FIRM
815 3rd Ave., S.
Fargo, ND 58103
Phone: 701-235-4481
Fax: 701-235-1107
scott@schneiderlawfirm.com

HELLMUTH & JOHNSON PLLC
Nathan D. Prosser
Anne T. Regan*
8050 West 78th Street
Edina, MN 55439
Phone: (952) 941-4005
nprosser@hjlawfirm.com
aregan@hjlawfirm.com

GUSTAFSON GLUEK PLLC
Daniel E. Gustafson
David A. Goodwin
Daniel J. Nordin*
Joe E. Nelson*
Canadian Pacific Plaza
120 South 6th Street, Suite 2600
Minneapolis, MN 55402
Phone: (612) 333-8844
dgustafson@gustafsongluek.com
dgoodwin@gustafsongluek.com
dnordin@gustafsongluek.com
jnelson@gustafsongluek.com

Interim Co-Lead Counsel for Plaintiffs and Putative Class

WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC
Carl V. Malmstrom
111 W. Jackson Blvd., Suite 1700
Chicago, Illinois 60604
Tel: (312) 984-0000
Fax: (212) 686-0114
malmstrom@whafh.com

CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
Nickolas J. Hagman
135 S. LaSalle, Suite 3210
Chicago, Illinois 60603
Minneapolis, MN 55401
Phone: (312) 782-4880
nhagman@caffertyclobes.com

CHESTNUT CAMBRONNE PA
Bryan L. Bleichner*
Philip J. Krzeski*
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Phone: (612) 339-7300
Fax: (612)-336-2940
bbleichner@chestnutcambronne.com
pkrzeski@chestnutcambronne.com

Counsel for Plaintiffs and the Putative Classes

* Pro Hac Vice Application Forthcoming